Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

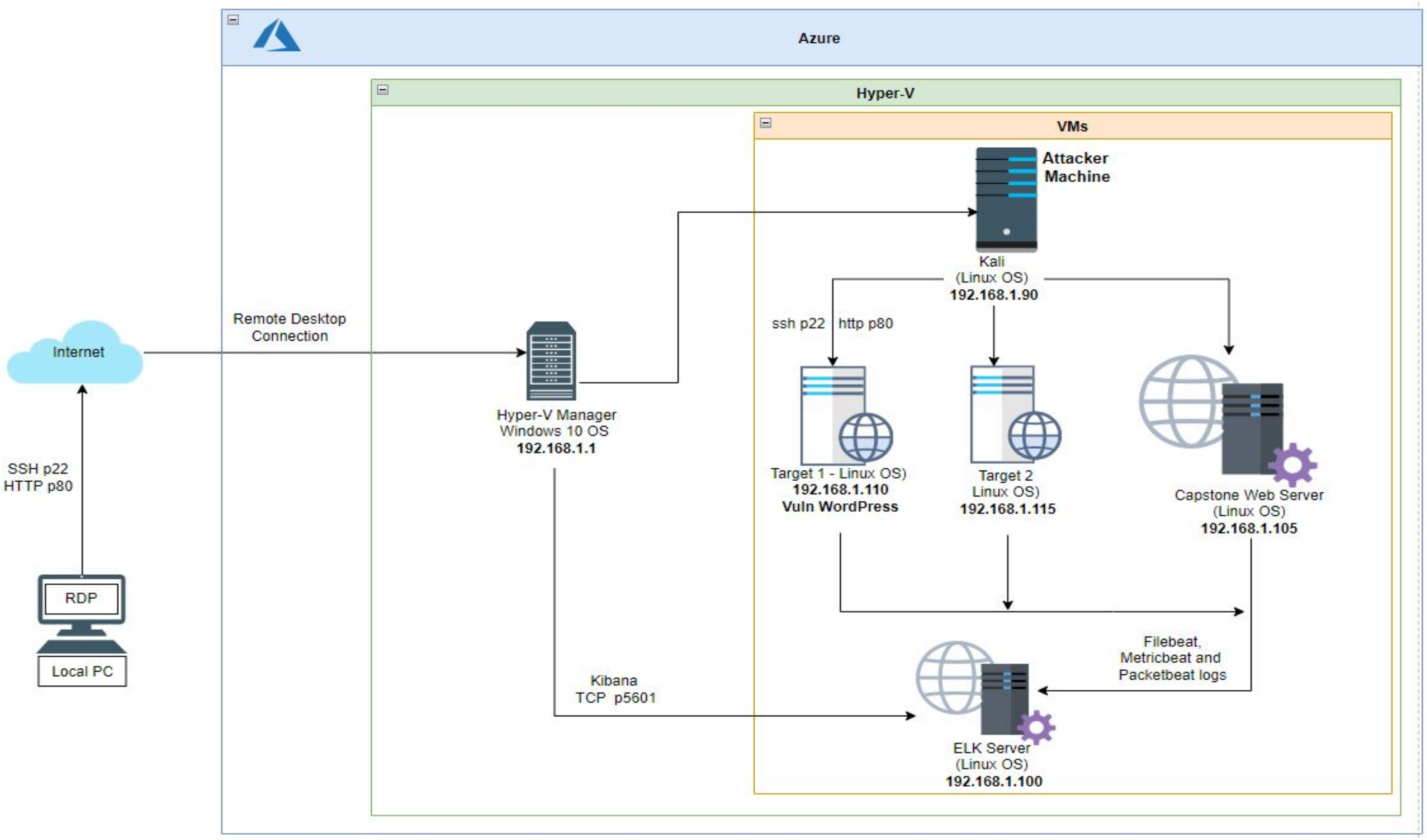
Andrew Nagy
Julio Ordonez
Tharsini Yogaratnam
Alexandra Wong
Brensley Edmondson
Kamran Maroussi

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask:255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4:192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.110
OS: Linux
Hostname: Target1

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	**Description**	**Impact**
Lack of perimeter protection against malware.	Perimeter protection would scan all inbound files for malware and viruses.	User was able to download malware from Internet.
Lack of endpoint protection against malware.	Endpoint protection would scan all inbound files for malware and viruses.	User was able to download and save malware from Internet.
Lack of perimeter white listing of Internet sites.	Perimeter protection would allow access to white listed websites and IP addresses.	User was able to visit IP address that is black listed according to https://www.ipvoid.com
Lack of protection against content outside of organization's acceptable use policy.	BitTorrent does not normally have a business requirement.	User was able to download torrent file.
Lack of password policy for Wordpress.	There appears to be no minimum requirements for password complexity, account timeouts etc.	A bad actor can brute force the admin login.
Poorly configured Wordpress Instance.	Lack of restrictions around file permissions, connecting to MySQL with Root.	Provides access to the SQL account credentials set within the wp_config.php file. Root account has full control of the database.
Sudo privileges to python	The user Steven has sudo access to python.	A bad actor can escalate privileges to root via python.

Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

Vulnerability	Description	Impact
phpMailer 5.2.17	Old version of software subject to CVE: 2016-10033. (https://packetstormsecurity.com/files/140280/PHPMailer-5.2.17-Remote-Code-Execution.html)	Able to launch a remote shell as web site user ‘www-data’.
Default content files left in place.	Some files contain configuration information.	Exposure of information to make reconnaissance easier.

Traffic Profile

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	1) 172.16.4.205 2) 10.0.0.201 3) 185.243.115.84	Machines that sent the most traffic.
Most Common Protocols	1) TCP(85.7%) 2) UDP(14.1%) 3) OTHER(0.02%)	Three most common protocols on the network.
# of Unique IP Addresses	1) 811	Count of observed IP addresses.
Subnets	1) 10.6.12.0/24 2) 172.16.4.0/24 3) 10.0.0.0/24	Observed subnet ranges.
# of Malware Species	1) june11.dll	Number of malware (trojan) binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

- Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Watching Youtube videos
- Looking into medical services
- Training Module/Trivia Game
- Looking into Bicycle Events and Cycling Tips

Suspicious Activity

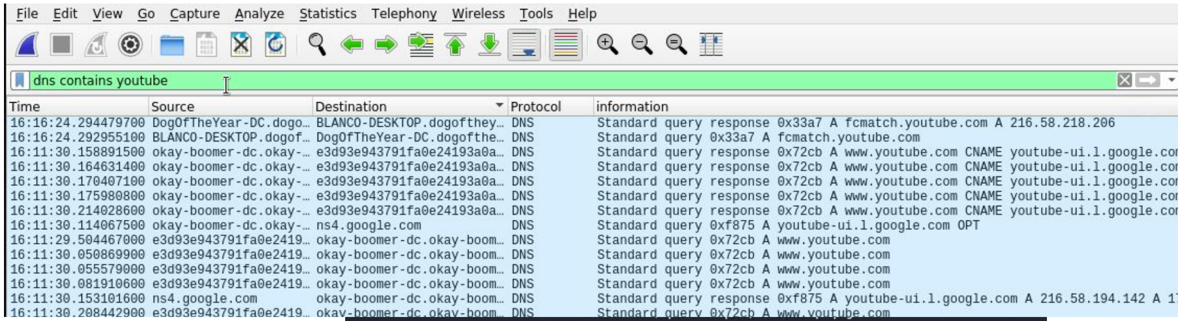
- Downloading Copyrighted Materials
- AD Server and Downloaded Malware
- Infected Windows Machine

Normal Activity

Normal #1: Watching Youtube videos

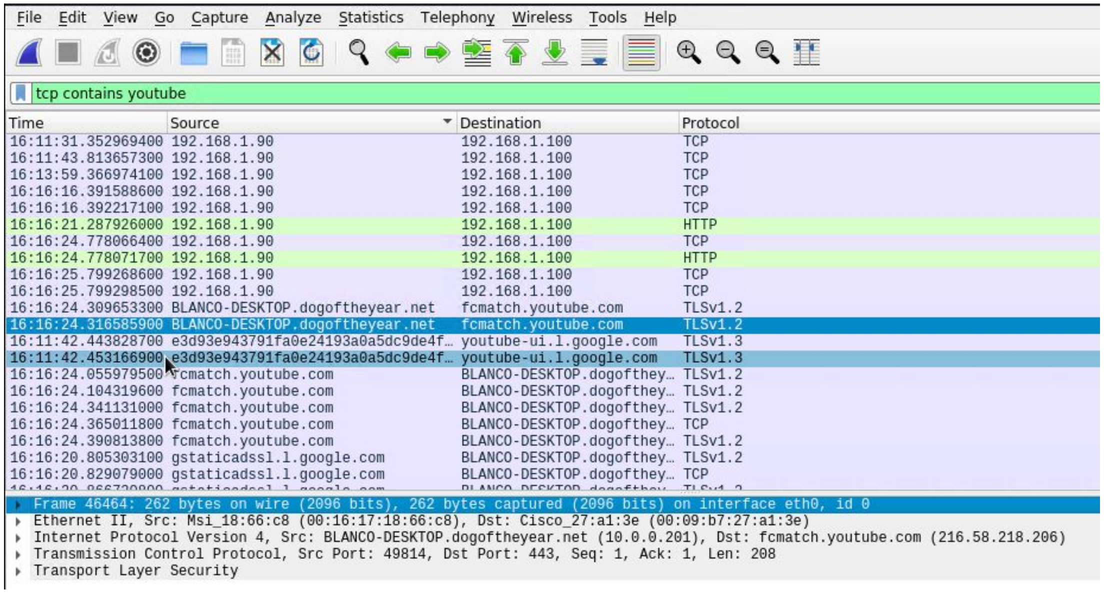
Summarize the following:

- What kind of traffic did you observe? Which protocol(s)? Transmission Control Protocol (TCP), TLSV1.2 (SSL Protocol), Domain Name Server (DNS)



dns contains youtube

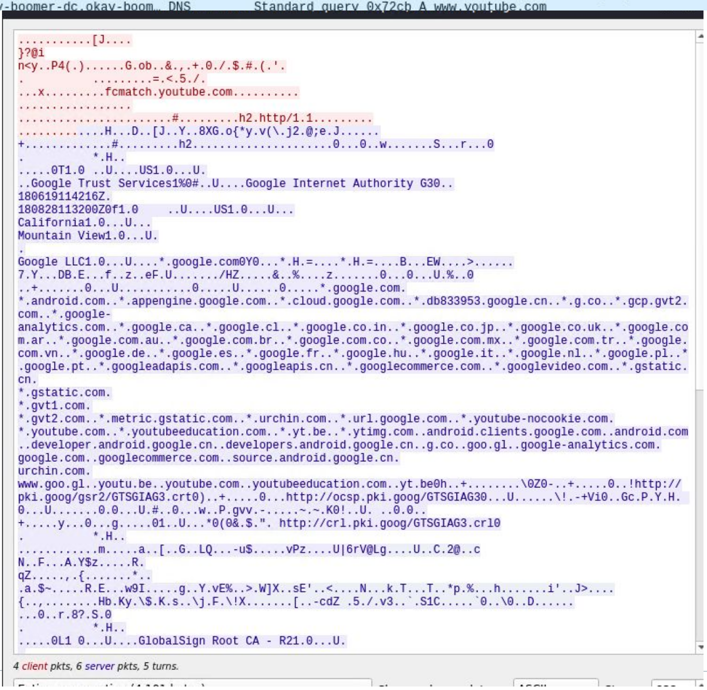
```
Time               Source                       Destination                  Protocol  information
16:16:24.294479700 DogOfTheYear-DC.dogo…        BLANCO-DESKTOP.dogofthey…    DNS       Standard query response 0x33a7 A fcmatch.youtube.com A 216.58.218.206
16:16:24.292955100 BLANCO-DESKTOP.dogof…        DogOfTheYear-DC.dogofthe…    DNS       Standard query 0x33a7 A fcmatch.youtube.com
16:11:30.158891500 okay-boomer-dc.okay-…        e3d93e943791fa0e24193a0a…    DNS       Standard query response 0x72cb A www.youtube.com CNAME youtube-ui.l.google.co
16:11:30.164631400 okay-boomer-dc.okay-…        e3d93e943791fa0e24193a0a…    DNS       Standard query response 0x72cb A www.youtube.com CNAME youtube-ui.l.google.co
16:11:30.170407100 okay-boomer-dc.okay-…        e3d93e943791fa0e24193a0a…    DNS       Standard query response 0x72cb A www.youtube.com CNAME youtube-ui.l.google.co
16:11:30.175980800 okay-boomer-dc.okay-…        e3d93e943791fa0e24193a0a…    DNS       Standard query response 0x72cb A www.youtube.com CNAME youtube-ui.l.google.co
16:11:30.214028600 okay-boomer-dc.okay-…        e3d93e943791fa0e24193a0a…    DNS       Standard query response 0x72cb A www.youtube.com CNAME youtube-ui.l.google.co
16:11:30.114067500 okay-boomer-dc.okay-…        ns4.google.com               DNS       Standard query 0xf875 A youtube-ui.l.google.com OPT
16:11:29.504467000 e3d93e943791fa0e2419…        okay-boomer-dc.okay-boom…    DNS       Standard query 0x72cb A www.youtube.com
16:11:30.050869900 e3d93e943791fa0e2419…        okay-boomer-dc.okay-boom…    DNS       Standard query 0x72cb A www.youtube.com
16:11:30.055579000 e3d93e943791fa0e2419…        okay-boomer-dc.okay-boom…    DNS       Standard query 0x72cb A www.youtube.com
16:11:30.081910600 e3d93e943791fa0e2419…        okay-boomer-dc.okay-boom…    DNS       Standard query 0x72cb A www.youtube.com
16:11:30.153101600 ns4.google.com               okay-boomer-dc.okay-boom…    DNS       Standard query response 0xf875 A youtube-ui.l.google.com A 216.58.194.142 A 1
16:11:30.208442900 e3d93e943791fa0e2419…        okay-boomer-dc.okay-boom…    DNS       Standard query 0x72cb A www.youtube.com
```



tcp contains youtube

```
Time               Source                                Destination                Protocol
16:11:31.352969400 192.168.1.90                          192.168.1.100              TCP
16:11:43.813657300 192.168.1.90                          192.168.1.100              TCP
16:13:59.366974100 192.168.1.90                          192.168.1.100              TCP
16:16:16.391588600 192.168.1.90                          192.168.1.100              TCP
16:16:16.392217100 192.168.1.90                          192.168.1.100              TCP
16:16:21.287926000 192.168.1.90                          192.168.1.100              HTTP
16:16:24.778066400 192.168.1.90                          192.168.1.100              TCP
16:16:24.778071700 192.168.1.90                          192.168.1.100              HTTP
16:16:25.799268600 192.168.1.90                          192.168.1.100              TCP
16:16:25.799298500 192.168.1.90                          192.168.1.100              TCP
16:16:24.309653300 BLANCO-DESKTOP.dogoftheyear.net       fcmatch.youtube.com        TLSv1.2
16:16:24.316585900 BLANCO-DESKTOP.dogoftheyear.net       fcmatch.youtube.com        TLSv1.2
16:11:42.443828700 e3d93e943791fa0e24193a0a5dc9de4f…     youtube-ui.l.google.com    TLSv1.3
16:11:42.453166900 e3d93e943791fa0e24193a0a5dc9de4f…     youtube-ui.l.google.com    TLSv1.3
16:16:24.055979500 fcmatch.youtube.com                   BLANCO-DESKTOP.dogofthey…  TLSv1.2
16:16:24.104319600 fcmatch.youtube.com                   BLANCO-DESKTOP.dogofthey…  TLSv1.2
16:16:24.341131000 fcmatch.youtube.com                   BLANCO-DESKTOP.dogofthey…  TLSv1.2
16:16:24.365011800 fcmatch.youtube.com                   BLANCO-DESKTOP.dogofthey…  TCP
16:16:24.390813800 fcmatch.youtube.com                   BLANCO-DESKTOP.dogofthey…  TLSv1.2
16:16:20.805303100 gstaticadssl.l.google.com             BLANCO-DESKTOP.dogofthey…  TLSv1.2
16:16:20.829079000 gstaticadssl.l.google.com             BLANCO-DESKTOP.dogofthey…  TCP
```

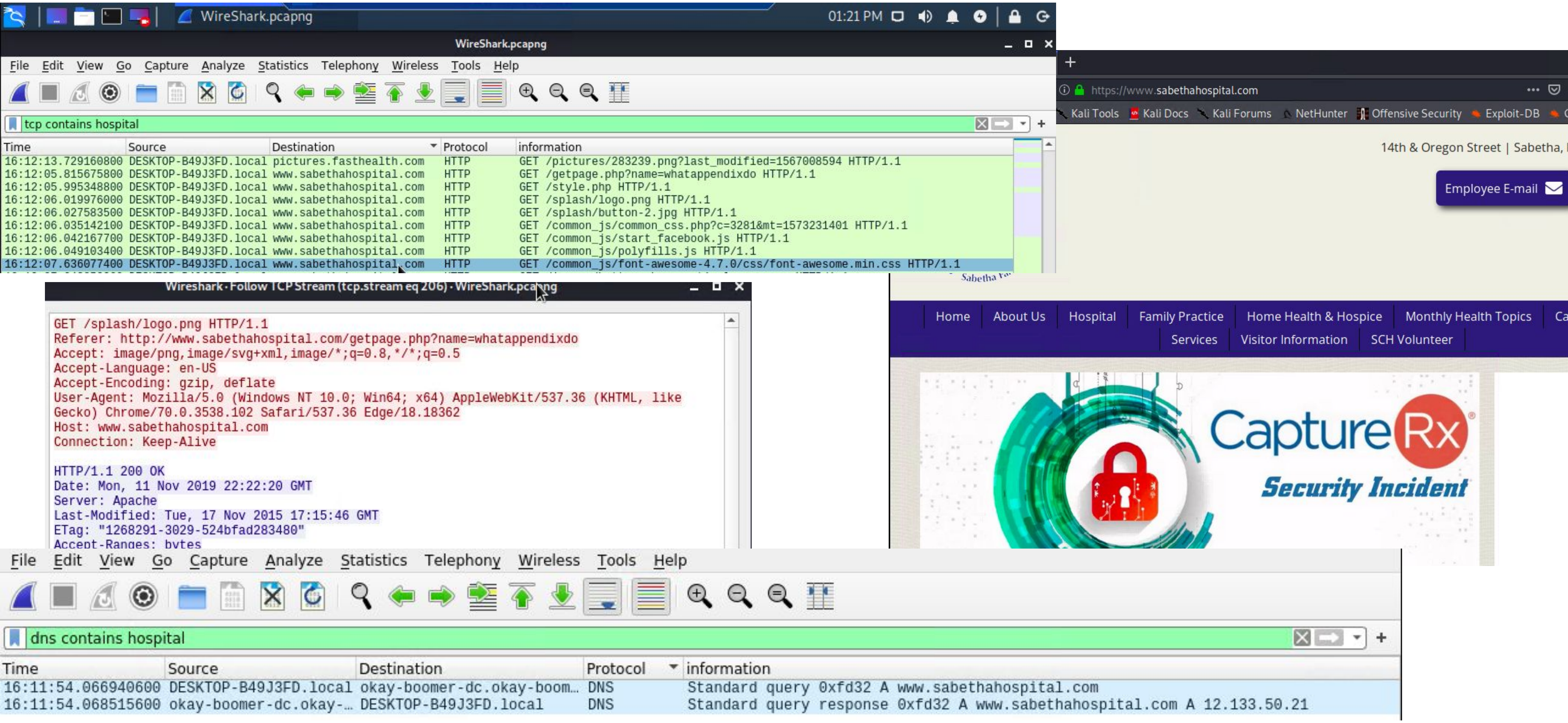
```
▸ Frame 46464: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits) on interface eth0, id 0
▸ Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
▸ Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: fcmatch.youtube.com (216.58.218.206)
▸ Transmission Control Protocol, Src Port: 49814, Dst Port: 443, Seq: 1, Ack: 1, Len: 208
▸ Transport Layer Security
```



```
...........[J....
}?@i
n<y..P4(.)......G.ob..&.,.+.0./.$.#.(.'.
.          .........=.<.5./.
...x.........fcmatch.youtube.com..........
.................
......................#.........h2.http/1.1.........
...............H...D..[J..Y..8XG.o{*y.v(\.j2.@;e.J......
+.............#.........h2.....................0...0..w.......S...r...0
.          *.H..
.....0T1.0 ..U....US1.0...U.
..Google Trust Services1%0#..U....Google Internet Authority G30..
180619114216Z.
180828113200Z0f1.0    ..U....US1.0...U...
California1.0...U...
Mountain View1.0...U.
.
Google LLC1.0...U....*.google.com0Y0...*.H.=....*.H.=....B...EW....>......
7.Y...DB.E...f..z..eF.U......./HZ.....&..%....z.......0...0...U.%..0
..+.......0...U...........0.....U......0.....*.google.com.
*.android.com..*.appengine.google.com..*.cloud.google.com..*.db833953.google.cn..*.g.co..*.gcp.gvt2.
com..*.google-
analytics.com..*.google.ca..*.google.cl..*.google.co.in..*.google.co.jp..*.google.co.uk..*.google.co
m.ar..*.google.com.au..*.google.com.br..*.google.com.co..*.google.com.mx..*.google.com.tr..*.google.
com.vn..*.google.de..*.google.es..*.google.fr..*.google.hu..*.google.it..*.google.nl..*.google.pl..*
.google.pt..*.googleadapis.com..*.googleapis.cn..*.googlecommerce.com..*.googlevideo.com..*.gstatic.
cn.
*.gstatic.com.
*.gvt1.com.
*.gvt2.com..*.metric.gstatic.com..*.urchin.com..*.url.google.com..*.youtube-nocookie.com.
*.youtube.com..*.youtubeeducation.com..*.yt.be..*.ytimg.com..android.clients.google.com..android.com
..developer.android.google.cn..developers.android.google.cn..g.co..goo.gl..google-analytics.com.
google.com..googlecommerce.com..source.android.google.cn.
urchin.com.
www.goo.gl..youtu.be..youtube.com..youtubeeducation.com..yt.be0h..+........\0Z0-..+.....0..!http://
pki.goog/gsr2/GTSGIAG3.crt0)..+.....0...http://ocsp.pki.goog/GTSGIAG30...U......\!.-+Vi0..Gc.P.Y.H.
0...U.......0.0...U.#..0...w..P.gvv.-.....~.~.K0!..U. ..0.0..
+.....y...0...g.....01..U...*0(0&.$.". http://crl.pki.goog/GTSGIAG3.crl0
.          *.H..
...........m.....a..[..G..LQ...-u$.....vPz....U|6rV@Lg....U..C.2@..c
N..F...A.Y$z.....R.
qZ.....,.{.......*..
.a.$~.....R.E...w9I.....g..Y.vE%..>.W]X..sE'..<....N...k.T...T..*p.%...h.......i'..J>....
{..,........Hb.Ky.\$.K.s..\j.F.\!X.......[..-cdZ .5./.v3..`.S1C.....`0..\0..D......
...0..r.8?.S.0
.          *.H..
.....0L1 0...U....GlobalSign Root CA - R21.0...U.
```

4 client pkts, 6 server pkts, 5 turns.

Normal #2: Looking into medical services



tcp contains hospital

```
Time               Source               Destination           Protocol  information
16:12:13.729160800 DESKTOP-B49J3FD.local pictures.fasthealth.com HTTP    GET /pictures/283239.png?last_modified=1567008594 HTTP/1.1
16:12:05.815675800 DESKTOP-B49J3FD.local www.sabethahospital.com HTTP    GET /getpage.php?name=whatappendixdo HTTP/1.1
16:12:05.995348800 DESKTOP-B49J3FD.local www.sabethahospital.com HTTP    GET /style.php HTTP/1.1
16:12:06.019976000 DESKTOP-B49J3FD.local www.sabethahospital.com HTTP    GET /splash/logo.png HTTP/1.1
16:12:06.027583500 DESKTOP-B49J3FD.local www.sabethahospital.com HTTP    GET /splash/button-2.jpg HTTP/1.1
16:12:06.035142100 DESKTOP-B49J3FD.local www.sabethahospital.com HTTP    GET /common_js/common_css.php?c=3281&mt=1573231401 HTTP/1.1
16:12:06.042167700 DESKTOP-B49J3FD.local www.sabethahospital.com HTTP    GET /common_js/start_facebook.js HTTP/1.1
16:12:06.049103400 DESKTOP-B49J3FD.local www.sabethahospital.com HTTP    GET /common_js/polyfills.js HTTP/1.1
16:12:07.636077400 DESKTOP-B49J3FD.local www.sabethahospital.com HTTP    GET /common_js/font-awesome-4.7.0/css/font-awesome.min.css HTTP/1.1
```

```
GET /splash/logo.png HTTP/1.1
Referer: http://www.sabethahospital.com/getpage.php?name=whatappendixdo
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362
Host: www.sabethahospital.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 11 Nov 2019 22:22:20 GMT
Server: Apache
Last-Modified: Tue, 17 Nov 2015 17:15:46 GMT
ETag: "1268291-3029-524bfad283480"
Accept-Ranges: bytes
```

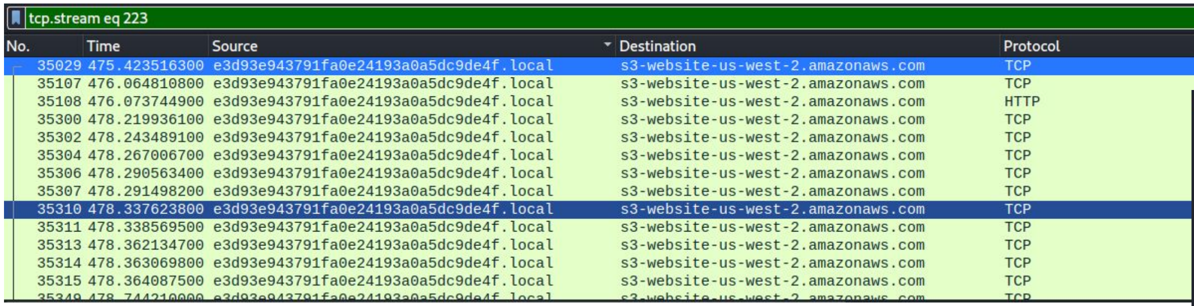
dns contains hospital

```
Time               Source                  Destination              Protocol  information
16:11:54.066940600 DESKTOP-B49J3FD.local   okay-boomer-dc.okay-boom… DNS      Standard query 0xfd32 A www.sabethahospital.com
16:11:54.068515600 okay-boomer-dc.okay-…   DESKTOP-B49J3FD.local    DNS      Standard query response 0xfd32 A www.sabethahospital.com A 12.133.50.21
```

Normal #3: Training Module/Trivia Game

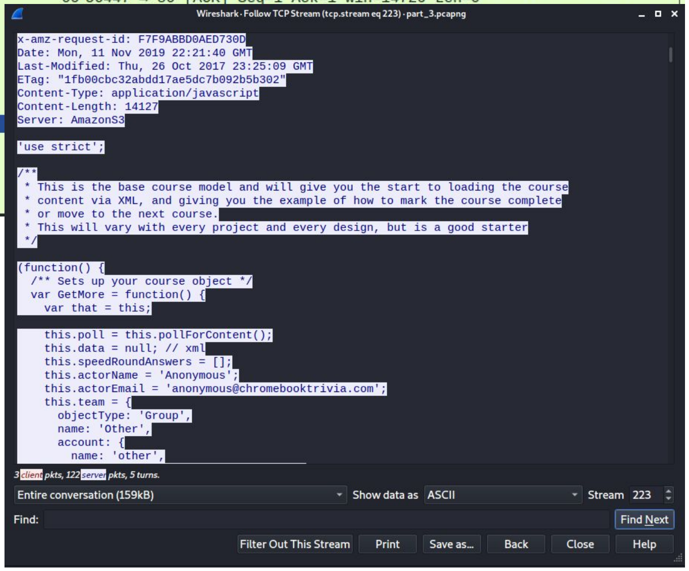
Summarize the following:

- Protocols used for this behaviour include TCP and HTTP, as seen in the screenshot below (initial filter used “tcp contains google”):



tcp.stream eq 223

No.	Time	Source	Destination	Protocol	Length	Info
35029	475.423516300	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP	74	56447 → 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=
35107	476.064810800	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP	60	56447 → 80 [ACK] Seq=1 Ack=1 Win=14720 Len=0
35108	476.073744900	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	HTTP		
35300	478.219936100	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP		
35302	478.243489100	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP		
35304	478.267006700	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP		
35306	478.290563400	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP		
35307	478.291498200	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP		
35310	478.337623800	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP		
35311	478.338569500	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP		
35313	478.362134700	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP		
35314	478.363069800	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP		
35315	478.364087500	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP		
35349	478.744210000	e3d93e943791fa0e24193a0a5dc9de4f.local	s3-website-us-west-2.amazonaws.com	TCP		



Wireshark · Follow TCP Stream (tcp.stream eq 223) · part_3.pcapng

```
x-amz-request-id: F7F9ABBD0AED730D
Date: Mon, 11 Nov 2019 22:21:40 GMT
Last-Modified: Thu, 26 Oct 2017 23:25:09 GMT
ETag: "1fb00cbc32abdd17ae5dc7b092b5b302"
Content-Type: application/javascript
Content-Length: 14127
Server: AmazonS3

'use strict';

/**
 * This is the base course model and will give you the start to loading the course
 * content via XML, and giving you the example of how to mark the course complete
 * or move to the next course.
 * This will vary with every project and every design, but is a good starter
 */

(function() {
  /** Sets up your course object */
  var GetMore = function() {
    var that = this;

    this.poll = this.pollForContent();
    this.data = null; // xml
    this.speedRoundAnswers = [];
    this.actorName = 'Anonymous';
    this.actorEmail = 'anonymous@chromebooktrivia.com';
    this.team = {
      objectType: 'Group',
      name: 'Other',
      account: {
        name: 'other',
```

3 client pkts, 122 server pkts, 5 turns.

Entire conversation (159kB) | Show data as: ASCII | Stream: 223

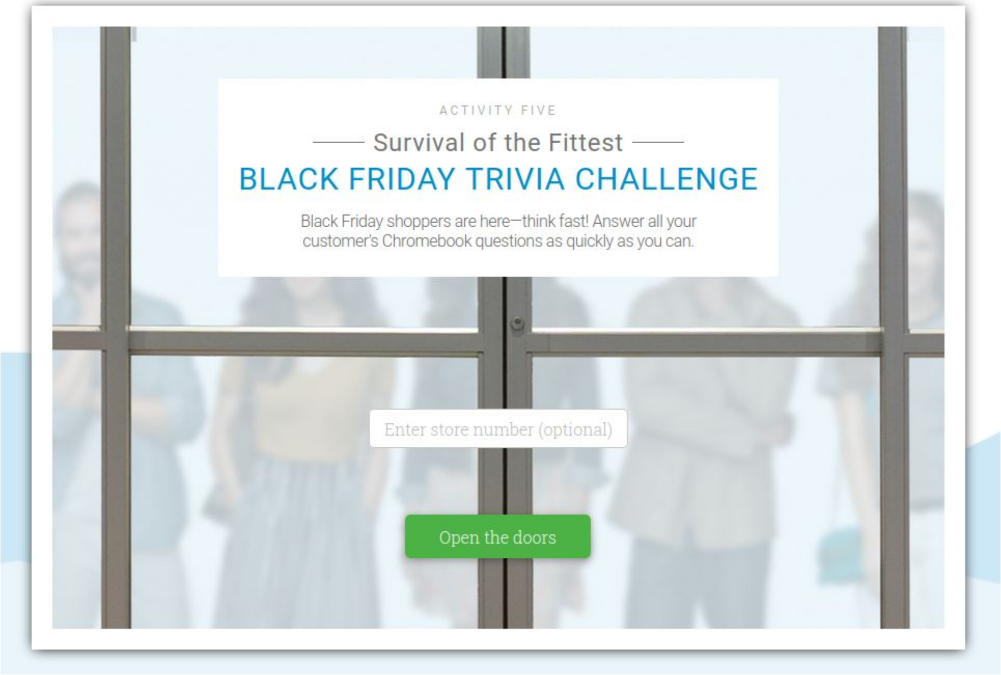
Find:

Upon following the TCP stream, we noticed the usage of TinCan API, which tracks the interactions of the user with the elements on screen, typical of modern eLearning modules, even though these interactions appeared to be tracked as an anonymous user.

Normal #3 (cont): Training Module/Trivia Game

Summarize the following:

- The user was accessed and interacted with a trivia challenge activity, located at http://www.chromebooktrivia.com. From the records, we can see that the server is located in AWS.



ACTIVITY FIVE

Survival of the Fittest

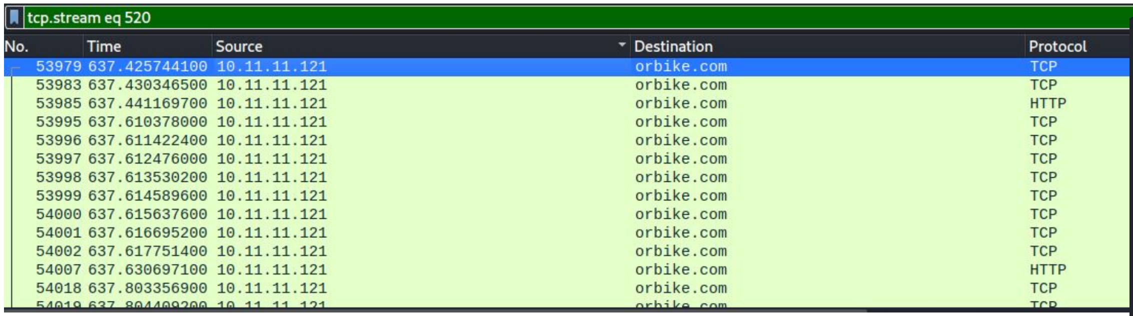
BLACK FRIDAY TRIVIA CHALLENGE

Black Friday shoppers are here—think fast! Answer all your customer's Chromebook questions as quickly as you can.

Normal #4: Looking into Bicycle Events and Cycling Tips

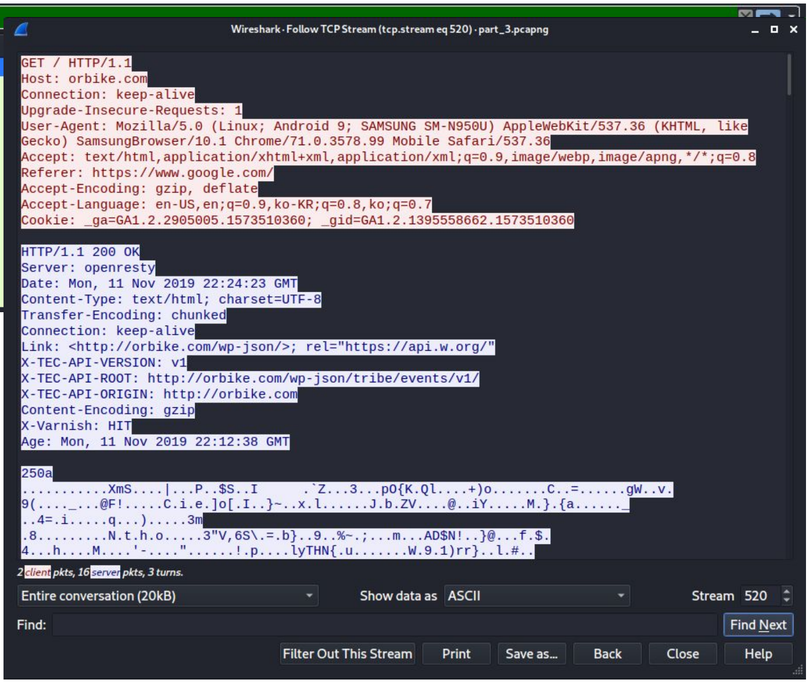
Summarize the following:

- Protocols used for this behaviour include HTTP and TCP, as seen in the screenshot below (initial filter used “tcp contains google”):



tcp.stream eq 520

```
No.    Time           Source          Destination    Protocol
53979 637.425744100 10.11.11.121    orbike.com     TCP
53983 637.430346500 10.11.11.121    orbike.com     TCP
53985 637.441169700 10.11.11.121    orbike.com     HTTP
53995 637.610378000 10.11.11.121    orbike.com     TCP
53996 637.611422400 10.11.11.121    orbike.com     TCP
53997 637.612476000 10.11.11.121    orbike.com     TCP
53998 637.613530200 10.11.11.121    orbike.com     TCP
53999 637.614589600 10.11.11.121    orbike.com     TCP
54000 637.615637600 10.11.11.121    orbike.com     TCP
54001 637.616695200 10.11.11.121    orbike.com     TCP
54002 637.617751400 10.11.11.121    orbike.com     TCP
54007 637.630697100 10.11.11.121    orbike.com     HTTP
54018 637.803356900 10.11.11.121    orbike.com     TCP
54019 637.804409200 10.11.11.121    orbike.com     TCP
```



Wireshark · Follow TCP Stream (tcp.stream eq 520) · part_3.pcapng

```
GET / HTTP/1.1
Host: orbike.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-N950U) AppleWebKit/537.36 (KHTML, like
Gecko) SamsungBrowser/10.1 Chrome/71.0.3578.99 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ko-KR;q=0.8,ko;q=0.7
Cookie: _ga=GA1.2.2905005.1573510360; _gid=GA1.2.1395558662.1573510360

HTTP/1.1 200 OK
Server: openresty
Date: Mon, 11 Nov 2019 22:24:23 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Link: <http://orbike.com/wp-json/>; rel="https://api.w.org/"
X-TEC-API-VERSION: v1
X-TEC-API-ROOT: http://orbike.com/wp-json/tribe/events/v1/
X-TEC-API-ORIGIN: http://orbike.com
Content-Encoding: gzip
X-Varnish: HIT
Age: Mon, 11 Nov 2019 22:12:38 GMT

250a
..........XmS....|...P..$S..I      .`Z...3...pO{K.Ql....+)o.......C..=......gW..v.
9(...._...@F!.....C.i.e.]o[.I..}~..x.l......J.b.ZV....@..iY.....M.}.{a......_
..4=.i.....q...).....3m
.8.........N.t.h.o.....3"V,6S\.=.b}..9..%~.;...m...AD$N!..}@...f.$.
4...h....M....'-...."......!.p....lyTHN{.u.......W.9.1)rr}..l.#..
```

2 client pkts, 16 server pkts, 3 turns.

Entire conversation (20kB)

Show data as: ASCII

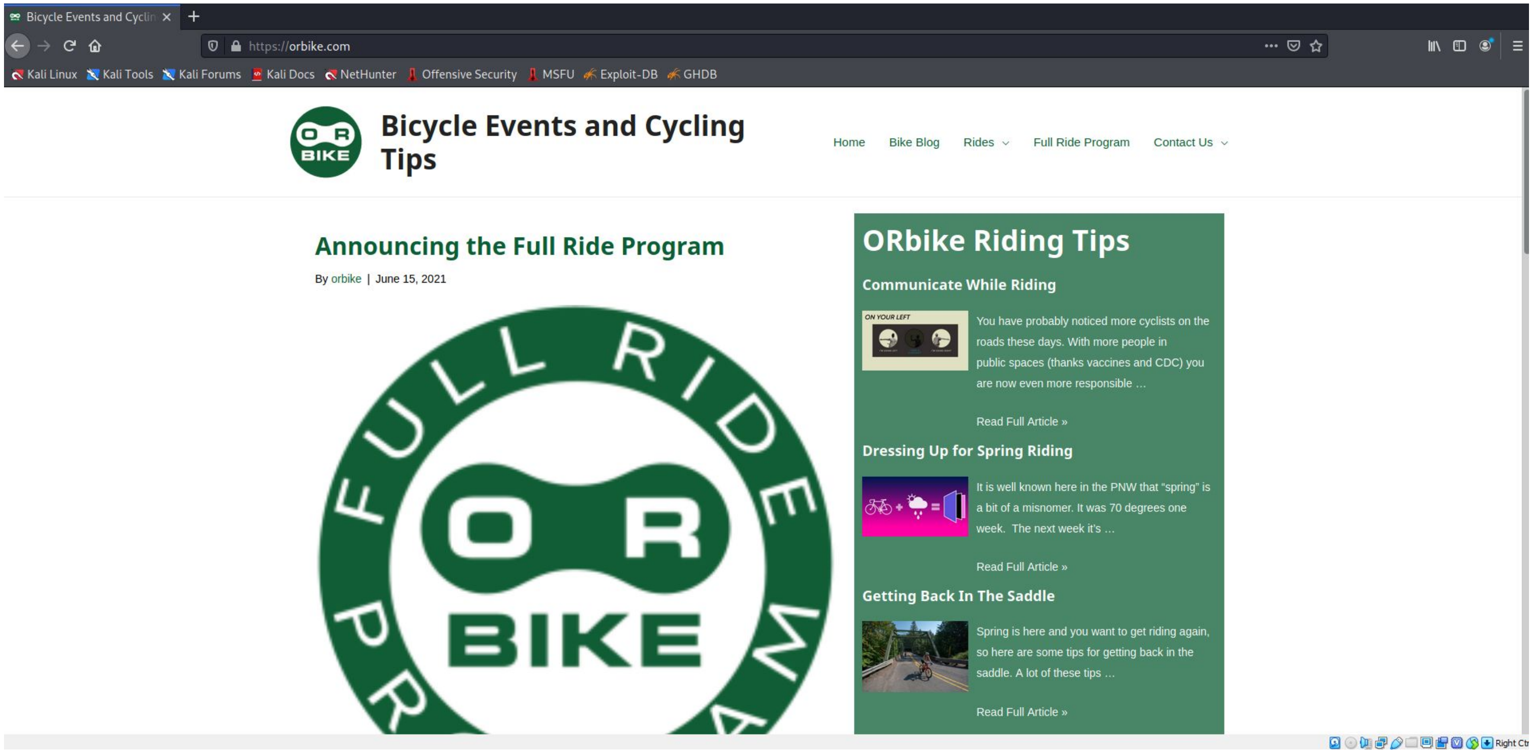
Stream: 520

Looking closer at the HTTP request, we can see that the user went to this page via Google as specified in the **Referer** field of the request.

Normal #4 (cont): Looking into Bicycle Events and Cycling Tips

Summarize the following:

- The user was browsing a Bicycle Events and Cycling tips, located at https://orbike.com



Bicycle Events and Cycling Tips

Announcing the Full Ride Program

By orbike | June 15, 2021

ORbike Riding Tips

Communicate While Riding

You have probably noticed more cyclists on the roads these days. With more people in public spaces (thanks vaccines and CDC) you are now even more responsible …

Read Full Article »

Dressing Up for Spring Riding

It is well known here in the PNW that "spring" is a bit of a misnomer. It was 70 degrees one week. The next week it's …

Read Full Article »

Getting Back In The Saddle

Spring is here and you want to get riding again, so here are some tips for getting back in the saddle. A lot of these tips …

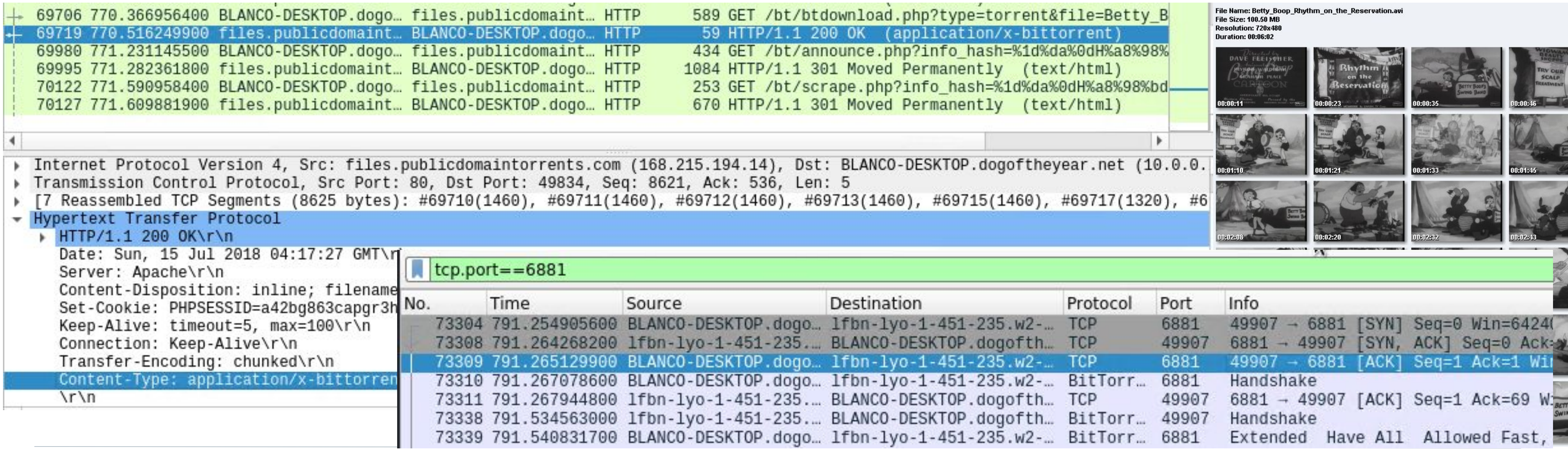
Read Full Article »

Malicious Activity

Malicious #1: Downloading Copyrighted Materials

Summarize the following:

- Torrent traffic was observed on the network (BitTorrent, TCP and HTTP protocols).
- The user was browsing through animated movies on http://publicdomaintorrents.info and downloaded one torrent file - “Betty Boop Rhythm on the Reservation.avi.torrent”.
- Packet 69706 is the HTTP GET request for the file, the response including the file is 69719.



```
69706 770.366956400 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP     589 GET /bt/btdownload.php?type=torrent&file=Betty_B
69719 770.516249900 files.publicdomaint… BLANCO-DESKTOP.dogo… HTTP      59 HTTP/1.1 200 OK  (application/x-bittorrent)
69980 771.231145500 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP     434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%
69995 771.282361800 files.publicdomaint… BLANCO-DESKTOP.dogo… HTTP    1084 HTTP/1.1 301 Moved Permanently  (text/html)
70122 771.590958400 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP     253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd
70127 771.609881900 files.publicdomaint… BLANCO-DESKTOP.dogo… HTTP     670 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
▸ Internet Protocol Version 4, Src: files.publicdomaintorrents.com (168.215.194.14), Dst: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 49834, Seq: 8621, Ack: 536, Len: 5
▸ [7 Reassembled TCP Segments (8625 bytes): #69710(1460), #69711(1460), #69712(1460), #69713(1460), #69715(1460), #69717(1320), #6
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Sun, 15 Jul 2018 04:17:27 GMT\r
    Server: Apache\r\n
    Content-Disposition: inline; filename
    Set-Cookie: PHPSESSID=a42bg863capgr3h
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Transfer-Encoding: chunked\r\n
    Content-Type: application/x-bittorren
    \r\n
```

File Name: Betty_Boop_Rhythm_on_the_Reservation.avi
File Size: 100.50 MB
Resolution: 720x480
Duration: 00:06:02

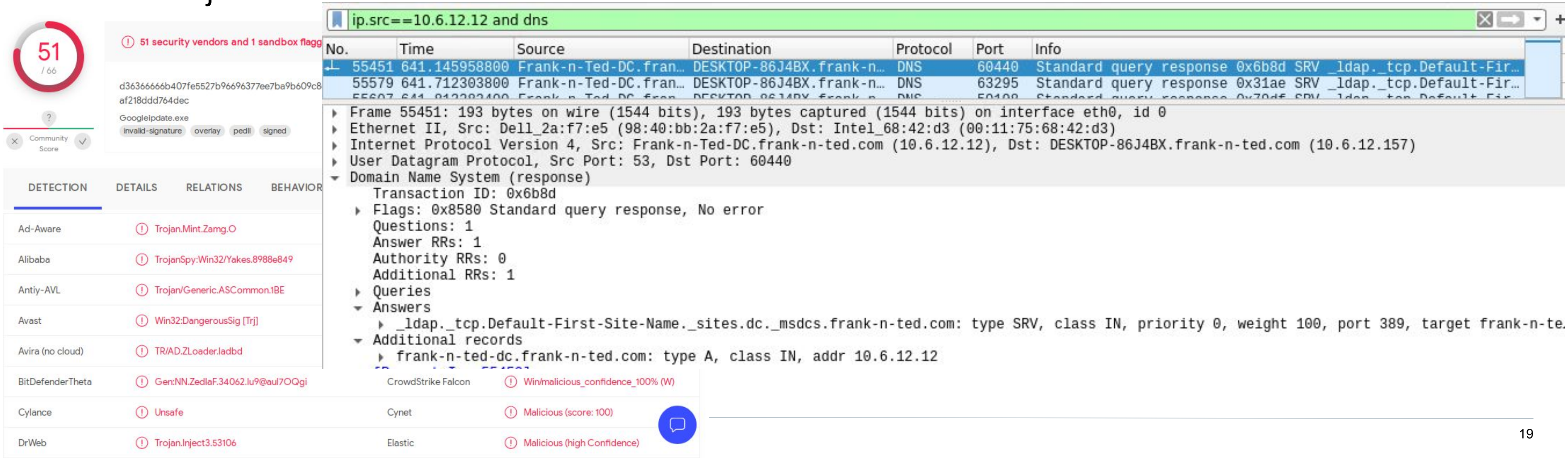
```
tcp.port==6881

No.    Time          Source                Destination           Protocol  Port   Info
73304 791.254905600 BLANCO-DESKTOP.dogo… lfbn-lyo-1-451-235.w2-… TCP       6881   49907 → 6881 [SYN] Seq=0 Win=6424(
73308 791.264268200 lfbn-lyo-1-451-235.… BLANCO-DESKTOP.dogofth… TCP       49907  6881 → 49907 [SYN, ACK] Seq=0 Ack=
73309 791.265129900 BLANCO-DESKTOP.dogo… lfbn-lyo-1-451-235.w2-… TCP       6881   49907 → 6881 [ACK] Seq=1 Ack=1 Wi
73310 791.267078600 BLANCO-DESKTOP.dogo… lfbn-lyo-1-451-235.w2-… BitTorr…  6881   Handshake
73311 791.267944800 lfbn-lyo-1-451-235.… BLANCO-DESKTOP.dogofth… TCP       49907  6881 → 49907 [ACK] Seq=1 Ack=69 W
73338 791.534563000 lfbn-lyo-1-451-235.… BLANCO-DESKTOP.dogofth… BitTorr…  49907  Handshake
73339 791.540831700 BLANCO-DESKTOP.dogo… lfbn-lyo-1-451-235.w2-… BitTorr…  6881   Extended  Have All  Allowed Fast,
```

Malicious #2: AD Network and Downloaded Malware

Summarize the following:

- Traffic related to a rogue Active Directory server has been observed. Protocols include LDAP, KRB5 (Kerberos), DNS.
- Two users created frank-n-ted.com (10.6.12.12).
- A client that was part of this domain downloaded a malware file called june11.dll. This file appears to be a Trojan.



51 security vendors and 1 sandbox flagg

d36366666b407fe5527b96696377ee7ba9b609c8
af218ddd764dec

Googleipdate.exe

Ad-Aware	Trojan.Mint.Zamg.O		
Alibaba	TrojanSpy:Win32/Yakes.8988e849		
Antiy-AVL	Trojan/Generic.ASCommon.1BE		
Avast	Win32:DangerousSig [Trj]		
Avira (no cloud)	TR/AD.ZLoader.ladbd		
BitDefenderTheta	Gen:NN.ZedlaF.34062.lu9@aul7OQgi	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Trojan.Inject3.53106	Elastic	Malicious (high Confidence)

ip.src==10.6.12.12 and dns

```
No.    Time           Source                 Destination              Protocol  Port   Info
55451  641.145958800  Frank-n-Ted-DC.fran…  DESKTOP-86J4BX.frank-n…  DNS       60440  Standard query response 0x6b8d SRV _ldap._tcp.Default-Fir…
55579  641.712303800  Frank-n-Ted-DC.fran…  DESKTOP-86J4BX.frank-n…  DNS       63295  Standard query response 0x31ae SRV _ldap._tcp.Default-Fir…
```

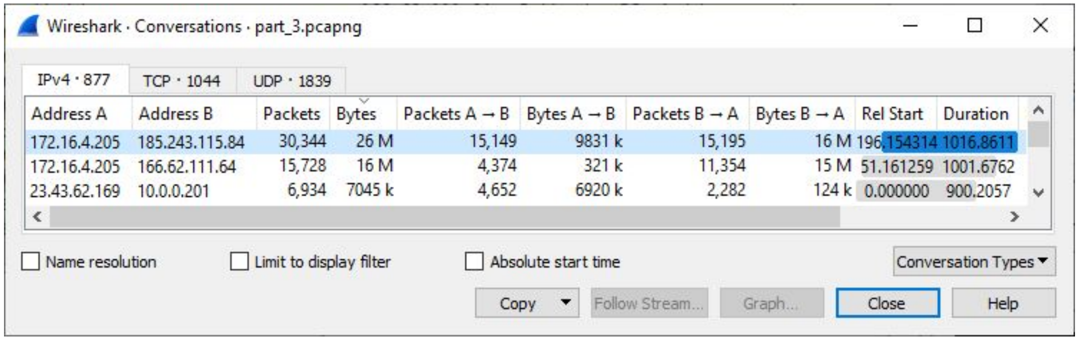
```
▸ Frame 55451: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface eth0, id 0
▸ Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Intel_68:42:d3 (00:11:75:68:42:d3)
▸ Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)
▸ User Datagram Protocol, Src Port: 53, Dst Port: 60440
▾ Domain Name System (response)
    Transaction ID: 0x6b8d
  ▸ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ Answers
    ▸ _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.frank-n-ted.com: type SRV, class IN, priority 0, weight 100, port 389, target frank-n-te.
  ▾ Additional records
    ▸ frank-n-ted-dc.frank-n-ted.com: type A, class IN, addr 10.6.12.12
```

Malicious #3: Infected Windows Machine

Summarize the following:

- What kind of traffic did you observe?
  Massive amount of traffic from
  185.243.115.84
  (b5689023.green.mattingsolutions.co)

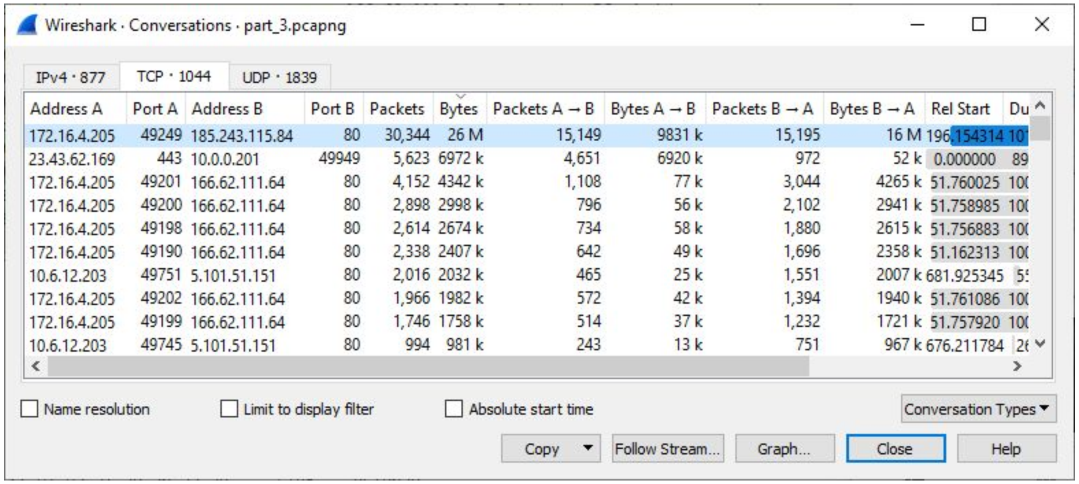
- Which protocol(s)?
  HTTP (tcp/80)



Wireshark · Conversations · part_3.pcapng

IPv4 · 877 | TCP · 1044 | UDP · 1839

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
172.16.4.205	185.243.115.84	30,344	26 M	15,149	9831 k	15,195	16 M	196.154314	1016.8611
172.16.4.205	166.62.111.64	15,728	16 M	4,374	321 k	11,354	15 M	51.161259	1001.6762
23.43.62.169	10.0.0.201	6,934	7045 k	4,652	6920 k	2,282	124 k	0.000000	900.2057



Wireshark · Conversations · part_3.pcapng

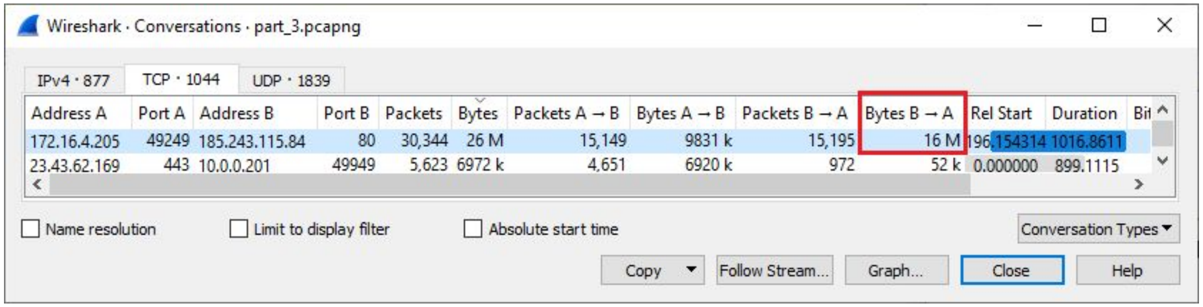
IPv4 · 877 | TCP · 1044 | UDP · 1839

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Du
172.16.4.205	49249	185.243.115.84	80	30,344	26 M	15,149	9831 k	15,195	16 M	196.154314	10
23.43.62.169	443	10.0.0.201	49949	5,623	6972 k	4,651	6920 k	972	52 k	0.000000	89
172.16.4.205	49201	166.62.111.64	80	4,152	4342 k	1,108	77 k	3,044	4265 k	51.760025	10
172.16.4.205	49200	166.62.111.64	80	2,898	2998 k	796	56 k	2,102	2941 k	51.758985	10
172.16.4.205	49198	166.62.111.64	80	2,614	2674 k	734	58 k	1,880	2615 k	51.756883	10
172.16.4.205	49190	166.62.111.64	80	2,338	2407 k	642	49 k	1,696	2358 k	51.162313	10
10.6.12.203	49751	5.101.51.151	80	2,016	2032 k	465	25 k	1,551	2007 k	681.925345	5
172.16.4.205	49202	166.62.111.64	80	1,966	1982 k	572	42 k	1,394	1940 k	51.761086	10
172.16.4.205	49199	166.62.111.64	80	1,746	1758 k	514	37 k	1,232	1721 k	51.757920	10
10.6.12.203	49745	5.101.51.151	80	994	981 k	243	13 k	751	967 k	676.211784	2

Malicious #3 (cont): Infected Windows Machine

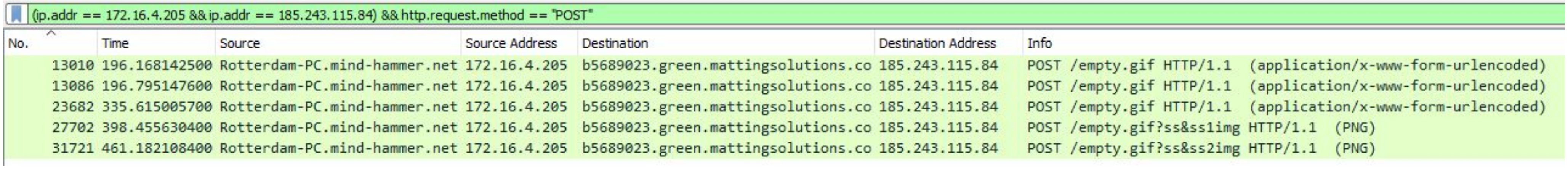
Summarize the following:

- What, specifically, was the user doing? Which site were they browsing? Downloading from 182.243.115.84



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bi
172.16.4.205	49249	185.243.115.84	80	30,344	26 M	15,149	9831 k	15,195	16 M	196.154314	1016.8611	
23.43.62.169	443	10.0.0.201	49949	5,623	6972 k	4,651	6920 k	972	52 k	0.000000	899.1115	

- Include screenshots of packets justifying your conclusions.



```
(ip.addr == 172.16.4.205 && ip.addr == 185.243.115.84) && http.request.method == "POST"
```

No.	Time	Source	Source Address	Destination	Destination Address	Info
13010	196.168142500	Rotterdam-PC.mind-hammer.net	172.16.4.205	b5689023.green.mattingsolutions.co	185.243.115.84	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
13086	196.795147600	Rotterdam-PC.mind-hammer.net	172.16.4.205	b5689023.green.mattingsolutions.co	185.243.115.84	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
23682	335.615005700	Rotterdam-PC.mind-hammer.net	172.16.4.205	b5689023.green.mattingsolutions.co	185.243.115.84	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
27702	398.455630400	Rotterdam-PC.mind-hammer.net	172.16.4.205	b5689023.green.mattingsolutions.co	185.243.115.84	POST /empty.gif?ss&ss1img HTTP/1.1 (PNG)
31721	461.182108400	Rotterdam-PC.mind-hammer.net	172.16.4.205	b5689023.green.mattingsolutions.co	185.243.115.84	POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)

- Include a description of any interesting files.
  - empty.gif would crash the Kali virtual machine when attempting to export it from Wireshark.

The End